5 FAM 1100
CLOUD COMPUTING

5 FAM 1110
CLOUD COMPUTING POLICY

(CT:IM-147; 09-10-2013)
(Office of Origin: IRM/BMP/SPO)

5 FAM 1111 SCOPE

(CT:IM-147; 09-10-2013)

a. The scope of this subchapter is the framework for development of Department of State operating and security standards for utilization of cloud computing.

b. This policy applies to all new and existing unclassified IT systems. Those unclassified systems that process information rated above FISMA Confidentiality rating of "Low" require approval by the Designated Approving Authority (DAA). (See 1 FAM 270 and 5 FAM 814.)

5 FAM 1112 AUTHORITIES

(CT:IM-147; 09-10-2013)

The authorities for this policy include:

(1) 25 Point Implementation Plan to Reform Federal IT;

(2) Federal Cloud Computing Strategy;

(3) NIST Special Publication 800-145, NIST Definition of Cloud Computing;

(4) NIST Special Publication 500-291, NIST Cloud Computing Standards Roadmap;

(5) NIST Special Publication 800-53, NIST Information Security;

(6) Information Security Guidelines for Secure Use of Cloud Computing by Federal Departments and Agencies Definitions;

(7) FedRAMP Policy Memo (OMB Memorandum December 8, 2011); and

(8) FedRAMP Concept of Operations.

5 FAM 1113 CLOUD COMPUTING EXPLAINED

5 FAM 1113.1 Definition

(CT:IM-147; 09-10-2013)

Cloud computing: The National Institute of Standards and Technology (NIST SP 800-145) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction."

The Federal Risk and Authorization Management Program (FedRAMP): A unified, government-wide risk management program focused on large outsourced and multi-agency systems. FedRAMP has been established to provide a standard approach to Assessing and Authorizing (A&A) cloud computing services and products. FedRAMP allows joint authorizations and continuous security monitoring services for U.S. Government and commercial cloud computing systems intended for multi-agency use. The objective of FedRAMP is threefold:

(1) To ensure that information systems/services used government-wide have adequate information security;

(2) To eliminate duplication of effort and reduce risk-management costs; and

(3) To enable rapid and cost-effective procurement of information systems/services for Federal agencies.

5 FAM 1113.2 Characteristics

(CT:IM-147; 09-10-2013)

The National Institute of Standards and Technology (NIST) outlines cloud computing characteristics as:

(1) **Five essential characteristics of cloud computing**: On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service;

(2) **Four cloud deployment models**: Cloud computing is defined to have several deployment models, each of which provides distinct trade-offs for agencies that are migrating applications to a cloud environment:

(a) **Private cloud**: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise;

(b) **Community cloud**: The cloud infrastructure is shared by several organizations and supports a specific community that has shared

concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise;

(c) **Public cloud**: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services; and

(d) **Hybrid cloud**: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds); and

(3) **Service models**: Service models may be provided for software, platform, or infrastructure:

(a) **Cloud software as a service (SaaS)**: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings;

(b) **Cloud platform as a service (PaaS)**: The capability provided to the consumer is the ability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations; and

(c) **Cloud infrastructure as a service (IaaS)**: The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

5 FAM 1114 CLOUD POLICY

(CT:IM-147; 09-10-2013)

a Cloud technologies enable information technology (IT) services to efficiently share demand across infrastructure assets, reducing the overall reserve capacity across the enterprise.

b. Department of State policy is to use cloud computing in order to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost.

c. Any proposed utilization of cloud solutions **must** adhere to FISMA and system owners are responsible for all applicable security requirements.

5 FAM 1115 USING CLOUD COMPUTING

(CT:IM-147; 09-10-2013)

a. All new Department IT projects **must** implement private, U.S. Government or public cloud computing technologies whenever cost effective, meet system/owner mission requirements, and provide the required level of security and performance. Compliance is monitored through the Department's Capital Planning Investment Control (CPIC) process. (See 5 FAM 610.)

b. System owners **must** conduct an analysis of cloud-service alternatives (see 5 FAM 1116, 5 FAM 610) to decide which cloud computing deployment should be used. Give preference to public cloud and U.S. Government-wide solutions and those that present the highest opportunity for Department IT savings. When public cloud deployment models are infeasible, use Department private-cloud solutions. All projects are encouraged to use cloud software as a service (SaaS) service model when commercially available. You **must** use cloud platform as a service (PaaS) or cloud infrastructure as a service (IaaS) when an SaaS solution is not available.

c. For existing projects, each system owner **must** evaluate the viability of migrating the legacy system to a cloud computing environment. Factors might include major system changes or improved cloud technologies.

d. Projects using public cloud offerings **must** select a FedRAMP-certified cloud service provider (CSP).

e. For all projects that are utilizing any cloud technology, the system owner **must** register this cloud instance in the Department's Information Technology Asset Baseline, or iTAB, database (see iTAB intranet site) for FISMA inventory and Office of Management and Budget (OMB) required reporting.

f. For all projects that are utilizing any cloud technology, the system owner **must** maintain a current backup of all data either in Department facilities or a third party unrelated to the primary cloud provider.

g. The Department maintains an effective incident response and mitigation capability for security and privacy incidents under cloud services, in accordance

with Federal policy and guidance. Project managers **must** require that cloud service providers route their traffic so that the provider's service meets the requirements of the Trusted Internet Connection (TIC) program.

5 FAM 1116 CLOUD COMPUTING ANALYSIS

(CT:IM-147; 09-10-2013)

When selecting applications for migration to a cloud environment, take the following into account:

(1) **Lifecycle**: If a legacy system is due to be replaced or undergo a major update within a year, a replacement system **must** consider a cloud solution;

(2) **Mission importance**: Migrate the least critical systems before mission-critical applications;

(3) **Information sensitivity**: Cloud solutions **must** meet security controls per National Institute of Standards and Technology (NIST) 800-53, FedRAMP, and Department standards;

(4) **Complexity**: Systems that are smaller or standalone (no interfaces to other systems) are prime candidates for migration;

(5) **Throughput or latency sensitivity**: Factor user experience into the analysis when evaluating systems that are bandwidth-intensive or delay-sensitive;

(6) **User population**: Systems which service external users (other Federal agencies, NGOs, and the public) are often prime candidates for a cloud; and

(7) **Costs**: The analysis should document the return on investment (ROI), including operational costs of cloud computing, both disclosed and hidden. Systems that realize an ROI within 3 years should be strongly considered for a cloud solution.

5 FAM 1117 THROUGH 1119 UNASSIGNED